

UNITED STATES DISTRICT COURT

for the  
Eastern District of Pennsylvania

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

A DARK IPHONE IN A DARK CASE, WITH IMEI  
NUMBER 350408489301177, SEIZED FROM  
MATTHEW HILL ON SEPTEMBER 26, 2023.

Case No. 24-MJ-475

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

A DARK IPHONE IN A DARK CASE, WITH IMEI NUMBER 350408489301177, SEIZED FROM MATTHEW HILL ON SEPTEMBER 26, 2023.

located in the Eastern District of Pennsylvania, there is now concealed (identify the person or describe the property to be seized):

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 922(g), 2199	Felon in possession of a firearm, carjacking

The application is based on these facts:  
See Affidavit

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Adam Cook

Applicant's signature

Adam Cook, Special Agent, FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
\_\_\_\_\_ telephone \_\_\_\_\_ (specify reliable electronic means).

Date: 03/18/2024

/s/ Richard A. Lloret

Judge's signature

City and state: Philadelphia, PA

Hon. Richard A. Lloret, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

IN THE MATTER OF THE SEARCH OF:  
  
A DARK COLORED IPHONE IN A DARK  
CASE, SEIZED FROM MATTHEW HILL  
ON SEPTEMBER 26, 2023.

Case No. 24-MJ-475

**Filed Under Seal**

**AFFIDAVIT OF PROBABLE CAUSE  
IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Adam Cook, hereby depose and state as follows:

1. I am a Special Agent with the FBI and have been so employed since December 2017. I am currently assigned to the Violent Crimes Task Force (VCTF) which investigates violations of federal law, including carjackings, robberies of banks, robberies of businesses that affect interstate commerce (also known as Hobbs Act robberies), and kidnappings. Furthermore, I have received training and experience as a police officer with the FBI Police for approximately four years prior to my current position as a Special Agent.

2. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended solely to demonstrate the existence of probable cause in support of the requested search warrant, and therefore does not set forth all of my knowledge and information about this matter.

3. This affidavit is submitted in support of a search warrant authorizing the search of an Apple iPhone with IMEI number 350408489301177 (the "SUBJECT PHONE").

**PROBABLE CAUSE**

4. On August 8, 2023 and September 18, 2023, Matthew HILL committed two carjackings in Philadelphia, PA by contacting his victims who were attempting to sell their cars

via Facebook Marketplace. HILL used a Facebook account with the name of “Mhizz Hill” to communicate with his victims. When HILL met the victims to see the vehicles, HILL produced a handgun and carjacked the vehicles.

5. On August 8, 2023, at approximately 1:14 PM, Philadelphia Police Department (PPD) Officers responded to 3300 S 61<sup>st</sup> Street, Philadelphia, PA for a reported carjacking. VICTIM 1 reported that he was attempting to sell a 2013 Chevrolet Impala that belonged to his business through Facebook Marketplace. This vehicle was taken from him at gunpoint by an individual later identified as Matthew HILL.

6. Prior to the meeting, VICTIM 1 corresponded through Facebook Marketplace with an account that used the name of “Mhizz Hill” in order to sell the Chevrolet Impala. VICTIM 1 set up a meeting with HILL on August 8, 2023, and HILL arrived at 3300 S 61<sup>st</sup> Street to see the Chevrolet Impala before purchasing it. When HILL arrived at the location, VICTIM 1 told HILL that the car was stored at another location: a car lot at 6221 W Passyunk Ave, Philadelphia, PA. HILL, VICTIM 1 and WITNESS 1 then went to 6221 W Passyunk Ave, Philadelphia, PA to see the car. After they arrived, HILL asked VICTIM 1 if he could take the car for a test drive and VICTIM 1 agreed. HILL got into the driver seat of the car and VICTIM 1 went with WITNESS 1 to open the gate to the car lot so that HILL could begin the test drive. As HILL drove toward them, he produced a black handgun and pointed it at VICTIM 1 and WITNESS 1. HILL told VICTIM 1 and WITNESS 1 not to follow him. HILL then fled the area in the carjacked Chevrolet Impala.

7. VICTIM 1 provided PPD Detectives with information concerning the Facebook Marketplace account for “Mhizz Hill,” which displayed a profile picture of the individual who met with VICTIM 1 and committed the carjacking. Detectives identified the individual in the account

as MATTHEW HILL, which appeared to be the same individual in Pennsylvania Driver's License Database photos.

8. PPD Detectives prepared and showed a photo array that included a photo of HILL to VICTIM 1; VICTIM 1 positively identified the photo of HILL as the individual that carjacked him.

9. On September 18, 2023, HILL committed another carjacking of a 2006 Dodge Durango from VICTIM 2 in the area of 1050 E Hunting Park Ave, Philadelphia, PA. On this date, VICTIM 2 met with HILL to sell VICTIM 2's Dodge Durango. VICTIM 2 set up the meeting through Facebook Marketplace with an account with the name of "Mhizz Hill." When VICTIM 2 met with HILL to show the car, HILL requested a test drive of the car. VICTIM 2 agreed to the test drive and got into the passenger seat of the car; HILL got into the driver's seat. At this time, HILL took out a black handgun and pointed it at VICTIM 2, and ordered VICTIM 2 out of the car. HILL then fled the area in the carjacked Durango.

10. PPD Detectives identified the common carjacking pattern and identified HILL as the subject in the second carjacking of the Dodge Durango. PPD Detectives prepared and showed a photo array to VICTIM 2 which contained HILL's photo. VICTIM 2 positively identified HILL as the individual that committed the carjacking of the Dodge Durango.

11. PPD Detectives obtained arrest warrants for carjacking and related charges for both carjackings.

12. On September 26, 2023, a PPD Officer observed the carjacked white Dodge Durango parked in the area of 1799 W Juniata Street, Philadelphia, PA; the PPD Officer knew of this carjacked Dodge Durango due to a Patrol Alert that had been issued within the PPD. The PPD Officer observed HILL enter the driver seat of the Durango and drive off. Aware of the recent

carjacking of the white Dodge Durango and the license plate on the Durango not matching a registration for a Dodge Durango, the PPD Officer conducted a traffic stop of the Dodge Durango. The PPD Officer then confirmed HILL's identify and the VIN of the carjacked Dodge Durango. HILL was arrested at this time and transported to PPD East Detectives. An Apple iPhone with IMEI number 350408489301177 was recovered in HILL's possession at the time of his arrest (the "SUBJECT PHONE"). The phone is a dark colored Apple iPhone with a dark colored case. The IMEI for the SUBJECT PHONE is the same device used in the call details records referenced later in this affidavit.

13. On September 26, 2023, PPD Detectives conducted a search of the Dodge Durango and recovered a black Polymer P-80 9 mm firearm in the vehicle.

14. After HILL was arrested for his active warrants, HILL was interviewed by PPD Detectives. HILL confirmed that his Facebook account used the name of "Mhizz." HILL stated that he bought the Dodge Durango from a person who he met on Facebook Marketplace. HILL denied stealing or carjacking any cars. HILL stated that he previously bought other cars on Facebook Marketplace, but HILL was not specifically asked about the car from the first carjacking in the interview.

15. PPD Detectives obtained cell phone records for HILL's phone, 267-357-6642. Analysis of his cell phone records showed that his cell phone was in the area of the Impala carjacking on August 8, 2023 from approximately 12:18 PM to 1:06 PM. For the Durango carjacking on September 18, 2023, the phone was in the area of that carjacking from approximately 7:05 PM to 7:33 PM.

16. Based on my review of court records, HILL has at least two prior felony convictions. Included in those court records were documents signed by HILL in which he

acknowledged that the crimes to which he was pleading guilty were punishable by more than one year in prison.

*Subject Phone*

17. SUBJECT PHONE is an Apple iPhone with IMEI number 350408489301177. There is probable cause to believe that HILL is the user of the SUBJECT PHONE because it was seized from him when he was arrested on September 26, 2023 while driving the stolen Dodge Durango.

18. After being seized, the SUBJECT PHONE was retained by the PPD.

19. In my training and experience, I know that the SUBJECT PHONE has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as it was when the SUBJECT PHONE first came into possession of law enforcement officers.

*Technical Terms*

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing

names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to

store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer



software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. **Tablet:** A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “wi-fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- g. **IP Address:** An Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- h. **Internet:** The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet,

connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

*Probable Cause to Search the Subject Phone for Items Described in Attachment B*

21. As discussed above, there is probable cause to believe that HILL has committed violations of Title 18 U.S.C. § 2119 (carjacking) and § 922(g) (unlawful possession of a firearm by a felon). There is probable cause to believe that the SUBJECT PHONE contains evidence of those crimes for the following reasons.

22. Based on my training, experience, and research, I know that the SUBJECT PHONE has capabilities that allows it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device and personal digital assistant (PDA). In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

23. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period on the device. This information can sometimes be recovered with forensics tools.

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT PHONE was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT PHONE because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).  
  
Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- c. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- d. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

25. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT

PHONE consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

26. Based on my training and experience, I know that individuals who commit carjackings often use their phones to take pictures of vehicles that are carjacked and communicate with others about the carjacked cars. For this specific case, I know that it would be likely for the subject to use his phone to communicate with the victims through Facebook Marketplace.

27. Based on my training and experience, individuals who illegally possess firearms often use their phones to send pictures of their firearms to their confederates and associates. Such individuals will often attempt to bolster their street reputation by sending pictures of their firearms, and/or messages about their firearms, to associates. For the same reason, individuals who illegally possess firearms often store pictures of their firearms on their phone.

**CONCLUSION**

28. I submit that this affidavit supports probable cause for a search warrant authorizing the search of Attachment A for the information described in Attachment B.

Respectfully submitted,

/s/ Adam Cook  
Adam Cook  
Special Agent  
Federal Bureau of Investigation

Telephonically subscribed and sworn to me on March 18, 2024.

/s/ Richard A. Lloret  
THE HONORABLE RICHARD A. LLORET  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

The property to be searched is a dark colored Apple iPhone in a dark case with IMEI number 350408489301177, which was seized from Matthew HILL on September 26, 2023 (the “SUBJECT PHONE”).

**ATTACHMENT B**

All records on the SUBJECT PHONE described in Attachment A that relate to a violation of Title 18 U.S.C. § 2119 (carjacking) and § 922(g) (unlawful possession of a firearm by a felon), involving Matthew HILL, including:

- a. All documents, to include in electronic form, and stored communications including contact information, pictures, text messages, call logs, voicemails, Internet searches, and any other electronic data or other memory features contained in the device described and SIM cards including correspondence, records, opened or unopened e-mails, text messages, and Internet history.
- b. All records relating to the ownership or use of the computer/phone equipment or devices.
- c. All records which evidence operation or ownership or use of the item described, including, but not limited to, correspondence, sales receipts, bills, financial records, tax records, personal photographs, telephone records, notebooks, diaries, reference materials, or other personal items, and registration information for any software on those items.
- d. During the course of the search, photographs of the Subject Cell Phone may also be taken to record the condition thereof and/or the location of items therein.
- e. All computer/phone passwords, keywords and other data security devices designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software, or other programming code. Any password or encryption key that may control access to a computer/phone operating system, individual computer/phone files, or other electronic data.
- f. Evidence and contents of logs and files on the items described, such as those generated by the phone's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted.
- g. Also, any malware resident on the computer/phone or device. Any information pertaining to the victims, and whereabouts that was transmitted, stored, or received using the applications or means described.
- h. Any data that would tend to show the identity of the person using the device.

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Pennsylvania

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

A DARK IPHONE IN A DARK CASE, WITH IMEI NUMBER  
350408489301177, SEIZED FROM MATTHEW HILL ON  
SEPTEMBER 26, 2023

Case No. 24-MJ-475

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Pennsylvania  
(identify the person or describe the property to be searched and give its location):

A DARK IPHONE IN A DARK CASE, WITH IMEI NUMBER 350408489301177, SEIZED FROM MATTHEW HILL ON SEPTEMBER 26, 2023.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Evidence of violations of 18 U.S.C. Sections 2119 (carjacking) and 922(g) (unlawful possession of a firearm by a felon).

**YOU ARE COMMANDED** to execute this warrant on or before \_\_\_\_\_ (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the duty magistrate.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_ .

Date and time issued: 03/18/2024 12:27 pm

/s/ Richard A. Lloret

Judge's signature

City and state: Philadelphia, PA

Hon. Richard A. Lloret, U.S. Magistrate Judge

Printed name and title



Case No.:  
24-MJ-475

Copy of warrant and inventory left with:

Inventory of the property taken and name of any person(s) seized:

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

---

*Executing officer's signature*

---

Printed name and title